UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,488	12/22/2005	Adrian Alvarez Diez	DE920030032US1	6307

30206 7590 10/27/2010

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
SHAW, PETER C	
ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
10/27/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

rociplaw@us.ibm.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/562,488
Filing Date: December 22, 2005
Appellant(s): DIEZ ET AL.

Grant A. Johnson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/11/2009 appealing from the Office action mailed 3/11/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20020152382	Xiao	10-2002
20060161975	Diez et al. (*as Admitted Prior Art taken from*	7-2006

PGPUB of application)

6,233,577	Ramasibramani et al.	5-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 12-16 are rejected under 35 U.S.C. 101 because the claimed inventions are directed to non-statutory subject matter. Claims 12-16 are considered functional descriptive material because the server and client components have not been limited to hardware in the specification (*See* Specification, Pages 8-10, "definition of claimed components").

Claims 1, 4-9, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao (US PGPUB No. 2002/0152382) [as cited in Information Disclosure Statement] in view of Applicant's Admitted Prior Art [hereinafter "AAPA"].

As per claim 1, Xiao teaches a method for validating and verifying a certificate by a client comprising:

receiving from said common database of said client system ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same

function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.) at least all necessary information of a third tier server certificate being accepted as trustworthy ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint),

comparing said received at least all necessary information with a server-copy of the third tier certificate received from said third tier server system (Fig. 2, 106, comparing thumbprints),

accepting said third tier server system as to be authenticated if said at least all necessary information certificate matches said server-copy of the third tier certificate (Fig. 2, 108, matched thumbprints; Fig. 2, 116, leads to authenticated server).

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 4, the combination of Xiao and AAPA teaches said at least all necessary information consisting essentially of a client-copy of said third tier server certificate as stored in the common data base of said distributed application environment, (Xiao, [0076], line 4, "A certified thumbprint" is all that is necessary to verify a received certificate.), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 5, the combination of Xiao and AAPA teaches at least all necessary information consisting essentially of a fingerprint of a client-copy of said third tier server (Xiao, [0076], line 4, "certificate thumbprint"), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 6, the combination of Xiao and AAPA teaches at least all necessary information consisting essentially of two different fingerprints of a client-copy of said third tier server (Xiao, [0076], line 4, "certificate thumbprint," It is implicit that the process can be performed multiple times for added security.), and a server name which has transmitted said client-copy of said third tier server certificate to said client system (Xiao, [0098], lines 24-25, "Associated trust information" includes the server name.).

As per claim 7, Xiao teaches a method comprising:

receiving a client-copy of a third tier server certificate from a third tier server system (Fig. 2, 102),

determining whether said received client-copy of said third tier server certificate can be accepted as trustworthy (Fig. 2, 122, Validation performed by root retrieving certificate.),

storing said client-copy of said third tier server certificate in said common data base of the distributed application environment if said client-copy of said third tier server certificate has been accepted as trustworthy ([0078], line 7-8, Updating the TIO involves storing thumbprints of certificates in its table.), and

transferring to each server of said server systems at least all necessary information of said client-copy of said third tier server certificates being accepted as trustworthy ([0088], lines 2-3, The hash values in the TIO are all that are necessary to validate a certificate.)

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 8, the combination of Xiao and AAPA teaches storing a name of said third tier server system that has transmitted said client-copy of said third tier certificate (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 9, the combination of Xiao and AAPA teaches said client-copy of said third tier server certificate is received via a secure transmission protocol (Xiao, [0004], line 1).

As per claim 16, Xiao teaches a client system comprising:

a connection negotiator component which, in a first computer process, receives incoming third tier server certificate via a secure connection from said third tier server ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.),

a common data base of the distributed application environment which, in a second computer process, stores said third tier server certificates received from said third tier server system which have been accepted as trustworthy for the distributed application environment ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.),

a certificate verifier component which, in a third computer process, compares said received third tier server certificate with information stored in said common

database and stores them into said common database if it matches (Fig. 2, 106, Hashing received certificate and comparing thumbprints.),

a certificate transmitter component which, in a fifth computer process, generates certificate information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database connection ([0076], lines 3-5, Database and TIO serve the same function of holding trusted certificates in the form of hashed thumbprints)and transmits them to said application server systems via a secure ([0088], line 2, The authentication information can be sent by a trusted server to the client.).

Xiao does not teach allowing for accepting or rejecting an unknown third tier server certificate not contained in said common data base, i.e. validating and later verifying the certificate. AAPA teaches allowing for accepting or rejecting an unknown third tier server certificate not contained in said common data base, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate([0013], lines 18-19).

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, allowing for accepting or rejecting an unknown third tier server certificate not contained in said

common data base, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

As per claim 17, the substance of the claimed invention is identical to that of claim 1. Accordingly, this claim is rejected under the same rationale.

Claims 2-3, 10-15, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao in view of AAPA and further in view of Ramasibramani et al. (US Patent No. 6,233,577) [hereinafter "Ramasubramani"].

As per claim 2, the combination of Xiao and AAPA teaches claim 1.

The combination of Xiao and AAPA does not teach said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection. However, Ramasubramani teaches said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection (Ramasubramani, Col. 7, line 64, "receiving/sending certificates").

At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine Xiao and AAPA, with the teachings of Ramasubramani, said at least all necessary receiving information from said client system is received via a non-continuous client-server connection, i.e. asynchronous connection, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 3, the newly added limitation(s) are identical to those introduced in claim 9. Accordingly, this claim is rejected under the same rationale.

As per claim 10, the newly added limitation(s) are identical to those introduced in claim 2. Accordingly, this claim is rejected under the same rationale.

As per claim 11, the combination of Xiao, AAPA, and Ramasubramani teaches authentication of said client system is accomplished by a user ID and/or password (Ramasubramani, Col. 7, lines 15-16).

As per claim 12, Xiao teaches a client system comprising:

a transfer server component, which in a first computer process, supports secure client-server connection ([0004], line 1), for receiving certificate information from a client of a third tier server certificates being accepted as trustworthy ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint)

a connection negotiator component which, in a second computer process receives incoming third tier server certificates (Fig. 2, 102) via a secure connection between said application server systems and said third tier server, ([0004], line 1)

a certificate verifier component, which in a third computer process, compares said third tier server certificate received from said third tier server with said certificate information received from client (Fig. 2, 106, comparing thumbprints).

Xiao does not teach determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate. AAPA teaches determining to accept or decline a connection to said third tier server system, i.e. validating ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, determining to accept or decline a connection to said third tier server system, i.e. validating and later verifying the certificate, to improve efficiency by limiting the amount of validation required.

The combination of Xiao and AAPA does not teach a non-continuous connection, i.e. asynchronous. Ramasubramani teaches a non-continuous connection, i.e. asynchronous (Col. 7, line 64, "receiving/sending certificates"). At the time of invention, it would have been obvious to one of ordinary skill in the art to combine Xiao and AAPA, with the teachings of Ramasubramani, a non-continuous connection, i.e. asynchronous, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 13, the combination of Xiao, AAPA, and Ramasubramani, teaches certificate information comprising two different fingerprints of the original third tier server certificate (Xiao, [0076], line 4, "certificate thumbprint," It is implicit that the process can be performed multiple times for added security.), name of the server which has transmitted said third tier server certificate to said client system, and certificate name (Xiao, [0098], lines 24-25, "Associated trust information" includes the server name and certificate name.).

As per claim 14, the combination of Xiao, AAPA, and Ramasubramani teaches said two different fingerprints generated by applying two different algorithms to said third tier server certificate received from said common database (Xiao, [0098]. line 15 and 34, "Algorithms" is recited in the plural, indicating at least two different algorithms. It is implicit that the process can be performed multiple times for added security.).

As per claim 15, the combination of Xiao, AAPA, and Ramasubramani teaches said application server systems including the same algorithms for generating the two different fingerprints (Xiao, [0098]. line 15 and 34, It is inherent that the system "includes" these algorithms.).

As per claim 18, the substance of the claim language is identical to that of claim 16. Accordingly, this claim is rejected under the same rationale.

As per claim 19, the substance of the claim language is identical to that of claim 12. Accordingly, this claim is rejected under the same rationale.

(10) Response to Argument

Appellant's Arguments (Brief, pages 11-15) have been fully considered but are not persuasive.

With respect to claims 12-16 rejected under 35 U.S.C. 101:

Appellant argues that claims 12-16 satisfy the "machine test" set forth in the Federal *Bilski* decision. To be considered statutory the invention in an apparatus or system claim may not be implemented by software alone. From the Examiner's understanding, the "machine test" set forth in the *Bilski* decision pertains solely to method claims. Examiner sees claims 12-16 as potentially comprising solely of software because the server and client components have not been limited to hardware in the specification (*See* Specification, Pages 8-10, "definition of claimed components"). The claims fail to establish a statutory category of invention, since the system is comprised solely of software components. Therefore, these claims were deemed non-statutory by the Examiner.

With respect to claim 1 rejected under 35 U.S.C. 103:

Appellant argues that the certification validation in the cited prior art Xiao is performed client-side and not server-side. Examiner submits that in combining Xiao with the admitted prior art, the Xiao reference is used to cover the certificate validation process. In Xiao, the client **receives** trust information (Xiao; Fig. 2, 102) and looks up reference trust information it has on file, i.e. thumbprints and if necessary root certificates (Xiao; Fig. 2, 106 and 118) and **compares** the trust information with the reference information (Xiao; Fig. 2, 106 and 118, comparing thumbprints or root certificates). The Examiner uses the admitted prior art to cover the structure of the third-tier system where the server-side now performs the certificate validation and **authenticates** the connection (Diez; Fig. 1; [0013], lines 14-19, server system performing certificate validation). The server can equally perform the certificate validation while performing the hashing. The end result of the combination would produce an authenticated connection as disclosed in the claimed invention. As far the elimination for the need of a local database, in Xiao, a TIO table (Xiao; [0063], lines 4-5, hash values of trusted certificates) and a trusted server (Xiao; Fig. 2, 118, storage of trusted certificates) act as the common database for which trusted reference information is stored. In conclusion, the combination of the admitted prior art with the disclosure in Xiao was used in the Examiner's rejection.

With respect to claims 7, 12 and 16 rejected under 35 U.S.C. 103:

The appellant's arguments are echoed and are covered by the above responses.

With respect to claims 2-6, 8-11, 13-15 and 17 rejected under 35 U.S.C. 103:

The appellant's arguments are echoed and are covered by the above responses.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Peter Shaw, Examiner

/P. S./
Examiner, Art Unit 2458

/Joseph E. Avellino/
Supervisory Patent Examiner, Art Unit 2458

/Benjamin R Bruckart/
Primary Examiner, Art Unit 2446